Ongoing Innovation

IIJ
Internet Initiative Japan

# libspf2脆弱性– TXT RR

Matsuzaki ‘maz’ Yoshinobu
<maz@iij.ad.jp>

# Sender Policy Framework (SPF)

- RFC4408 - 送信元認証
  - メール送信元がメール送信のポリシを記述
    - @example.comのメールは特定ホストから送出等
  - うまくやれば、送信元ドメインを偽装したメールを識別できる
- 実装が簡単
  - 保持しているドメインにTXTレコードを記述する

# 記述例

- iij.ad.jp

  IN TXT "v=spf1 ip4:210.138.77.20/30
  ip4:202.232.30.145 ip4:202.232.30.71
  ip4:210.138.77.13 ip4:210.138.145.126
  ip6:2001:240:11e:6000::1:145
  ip6:2001:240:11e:6300::1:71 -all”

- securemx.jp

  IN TXT "v=spf1 ip4:210.138.77.20/30 ~all"

# TXTレコードの悪用

- DNS amplification attack
  - 巨大なレコードを生成するのに利用されていた
- 比較的自由にレコード長を弄れる
  - なんせ書き放題

- 嫌な予感。。。。

# JVNVU#183657

- **libspf2 の DNS TXT レコード解析処理におけるバッファオーバーフローの脆弱性**
  - 2008年11月5日発表
  - http://jvn.jp/cert/JVNVU183657/index.html
  - libspf2 1.2.8より前のバージョン
- 巨大なtxtレコードが記述されているとダメ
  - heap-baseのバッファオーバーフローで、何らかのコードを実行されてしまう危険性

# 対策

- libspf2を利用している場合は、1.2.8以降のバージョンへアップグレード
  - 2008/11/25時点で1.2.9が最新版の様です

# 心にとどめておくこと

- DNSの大らかさは、万物を包み込む
  - 異常なレコード
  - 予期せぬ記述
- 想定したレコードが来ないこともある

- 何にせよ、libspf2を利用されている場合には速やかに1.2.8以降に更新を

# おわり